DISPOSITIF ET PROCEDE DE CONTROLE D'ACCES A DES RESSOURCES

La présente invention concerne un dispositif et un procédé de contrôle d'accès à des ressources d'un système informatique.

L'art antérieur

Les systèmes informatiques disposant d'un très grand nombre de ressources réparties géographiquement nécessitent désormais de nombreux administrateurs pour leur gestion. Chaque administrateur est propriétaire de droits d'exécution de commandes privilégiées sur des ressources déterminées.

Un problème posé par l'invention est de contrôler les droits des administrateurs dans un système informatique et d'empêcher ceux qui n'ont pas reçu l'autorisation adéquate d'effectuer des actions sur des ressources données.

De plus, le nombre de ressources dans un système informatique s'accroît rapidement. De ce fait, le contrôle d'accès est rendu complexe compte tenu du nombre important d'informations à gérer.

Actuellement, pour répondre à de tels problèmes, les systèmes informatiques comprennent au niveau de chacune des ressources gérées une liste de contrôle d'accès spécifiant les droits d'administrateurs ou de groupes d'administrateurs identifiés, d'effectuer une action donnée sur la ressource concernée. Les droits des administrateurs ou groupes d'administrateurs sont précisés ressource par ressource. La liste des droits associés à une ressource est enregistrée dans un fichier associé à ladite ressource. Lorsqu'une application lancée par un administrateur donné souhaite accéder à une ressource, le système consulte la liste qui est

rattachée à la dite ressource et vérifie si ledit administrateur a le droit d'y accéder.

Un tel système est basé sur l'identité de l'administrateur et plus le nombre d'administrateurs augmentent, plus le système se complexifie, plus il devient lent et coûteux. Par ailleurs, le système nécessite d'accéder à la ressource interrogée même si l'administrateur appelant n'a pas les droits suffisants requis pour ce faire et que la demande de l'administrateur est finalement rejetée. Il en résulte un temps de réponse important.

Un but de la présente invention consiste à simplifier le procédé de contrôle d'accès à des ressources d'un système.

Un autre but de l'invention est d'éviter l'accès systématique aux ressources interrogées pour vérifier les droits de l'appelant et autoriser l'accès auxdites ressources.

Résumé de l'invention

Dans ce contexte, la présente invention propose un procédé de contrôle d'accès d'un demandeur à des ressources dans un système informatique, caractérisé en ce qu'il consiste à définir des rôles recouvrant un ou plusieurs privilèges et représentant une compétence du demandeur pour réaliser des tâches spécifiques, à enregistrer les rôles définis dans des moyens de stockage, et à enregistrer une liste de contrôle d'accès définissant les conditions d'obtention d'un droit sur un type de ressource, à savoir d'une permission configurée en terme de privilèges dans lesdits moyens.

La présente invention concerne également le système de mise en œuvre dudit procédé.

Présentation des figures

D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description qui suit, donnée à titre d'exemple illustratif et non limitatif de la présente invention, en référence aux dessins annexés dans lesquels:

- la figure 1 est une vue schématique d'une forme de réalisation du système selon l'invention ;
- la figure 2 représente une forme de réalisation de la liste représentée sur le figure 1 ;
- la figure 3 est un exemple de la liste représentée sur la figure 2.
- la figure 4 est un tableau d'exemples de groupes génériques de droits et ressources.

Description d'une forme de réalisation de l'invention

Le système informatique peut être un système dont l'environnement est de type distribué ou local.

Comme le montre la forme de réalisation du système selon l'invention illustrée sur la figure 1, le système informatique 1 est distribué et composé de machines 2a, 2b, 2c, 2d organisées en un ou plusieurs réseaux 3. Une machine 2 est une unité conceptuelle très large, de nature matérielle et logicielle. Les machines peuvent être très diverses, telles que des stations de travail, serveurs, routeurs, machines spécialisées et passerelles entre réseaux. Seuls les composants des machines 2 du système 1 caractéristiques de la présente invention seront décrits, les autres composants étant connus de l'homme du métier.

Comme le montre la figure 1, dans la présente invention, le système informatique 1 comprend au moins une machine 2a dite machine 2a cliente, au moins une machine 2b de stockage de sécurité centralisée, au moins un serveur 2c d'administration, au moins une machine 2d de ressource administrée. Il est à noter que les machines 2 sont susceptibles d'être regroupées les unes aux autres, ainsi par exemple, la machine 2b de stockage et le serveur 2c d'administration peuvent ne former qu'une seule machine.

La ressource 2d est entendue au sens large, à savoir toute entité, logique et/ou physique, accédée et manipulée par des machines 2a cliente. La ressource se présente à titre illustratif sous la forme d'une imprimante, un fichier... La ressource 2d est, dans l'exemple décrit, caractérisée par un type, et éventuellement un identifiant. Un type de ressource regroupe un ensemble de droits qui s'appliquent à toutes les ressources de ce type. L'identifiant est constitué par exemple par un nom, un chemin d'accès...

A titre illustratif, la ressource 2d est une imprimante de type « imprimante réseau » et ayant pour identifiant le chemin de la ressource « \\mao.dom\bleuet ». Selon un autre exemple, la ressource 2d est une base de données de facturation de Louveciennes de type « base de données » ayant pour identifiant le nom de la base de données « database_facturation.frlv.bull.fr ». Le type « base de données » regroupe par exemple les droits suivants : « démarrer », « arrêter », « configurer », etc.

Un critère de contrôle d'accès est une propriété de la ressource 2d utilisée pour réaliser le contrôle d'accès sur cette ressource. Le critère identifie de manière unique une ressource particulière ou un ensemble de ressources. Les propriétés de la ressource susceptibles d'être utilisées comme critères sont par exemple le type de la ressource, le chemin ou la combinaison des deux.

La machine 2a cliente comprend au moins une entité 4 appelante, une interface 5 de programmation applicative (API), un service 6 de contrôle d'accès (appelé RAC). L'entité 4 appelante, l'API 5 et le RAC 6 sont susceptibles de faire partie d'une unique machine 2 ou de machines 2 différentes.

L'entité 4 appelante représente dans ce qui suit toute entité logique et/ou physique effectuant un ensemble de procédures et traitements et susceptibles de nécessiter l'accès à une ou plusieurs ressources 2d. L'entité 4 appelante se présente par exemple sous la forme d'une application, un fichier, une commande.

Un demandeur 7 lance l'entité 4 appelante et requiert l'autorisation d'effectuer une action dans le cadre de cette entité 4 sur une ressource 2d. Le demandeur 7 est une personne physique et dans la forme de réalisation illustrée un administrateur. Dans exemple illustré, l'entité 4 appelante se présente sous la forme d'une application et la ressource 2d d'une base de données : la machine 2a cliente traite la question de savoir si l'administrateur 7 opérant sur ladite application 4 a le droit d'effectuer une action sur une base de données 2d. Le demandeur ne peut accéder à ladite ressource 2d que si il dispose de droits suffisants.

Un droit désigne une ou plusieurs actions ou commandes effectuées par un demandeur 7 dans le contexte d'une entité 4 appelante, d'une ressource 2d ou d'un ensemble de ressources 2d. Pour un demandeur 7, le droit est global ou spécifique à une ressource 2d, et dans ce dernier cas, il définit un type d'accès particulier à la ressource 2d concernée. Par exemple, dans le contexte de bases de données, un administrateur peut avoir le droit d'arrêter ou de démarrer des bases de données particulières selon son rôle et ses privilèges d'administration.

L'entité 4 appelante reçoit de demandeurs 7 des requêtes d'accès à des ressources 2d. Selon une forme de réalisation particulière, l'entité 4 appelante offre au demandeur 7 une interface graphique 8 par l'intermédiaire de laquelle le demandeur 7 saisit sa requête. L'API 5 transmet l'interrogation de l'entité 4 appelante au RAC 6. L'API 5 fait l'interface entre l'entité 4 appelante et le RAC 6 auquel elle est associée. Le RAC 6 contrôle l'accès des demandeurs 7 aux ressources 2d interrogées.

L'API 5 offre notamment des fonctions d'accès au RAC notamment pour la prise de décision en réponse à la question posée par l'entité 4 appelante.

Le RAC 6, comme le montre la figure 1, comporte trois modules fonctionnels :

- un module 9 d'accès à des moyens 10 de stockage et plus particulièrement dans la présente forme de réalisation, à des moyens 10 d'enregistrement de rôles, privilèges et domaines de validité du demandeur qui seront définis dans ce qui suit ;
- un module 11 d'accès à des moyens 12 de stockage, et plus particulièrement dans la présente forme de réalisation, à des moyens 12 d'enregistrement de listes de contrôle d'accès des demandeurs permettant de charger les listes de contrôle d'accès se présentant sous la forme de fichiers, ou autres moyens de stockage ; le module 11 est appelé dans ce qui suit le RAD.
- un moteur 13 d'autorisation.

Le système selon la présente invention est basé sur une caractéristique particulière des demandeurs 7, à savoir leur rôle dans l'entreprise, et plus particulièrement (exemple illustré) dans l'administration des systèmes informatiques de l'entreprise. Pour définir le rôle d'un demandeur, il est tout d'abord nécessaire d'expliciter ce que représente un privilège.

Un privilège est un attribut de sécurité d'un demandeur 7 pour permettre le contrôle d'accès de ce dernier à des ressources 2d. Chaque ressource dispose d'une liste propre de privilèges ; il est également susceptible de prévoir des listes de privilèges communs à plusieurs ressources ou à tout le système. Le privilège est attribué à un demandeur directement ou indirectement par l'intermédiaire d'un rôle. Par exemple, un administrateur peut se voir attribuer le privilège « admin_db » d'administrateur de base de données, privilège qui lui permet de démarrer tout type de base de données (figure 3).

Un rôle est constitué d'un ensemble de privilèges : il recouvre une connotation métier et représente une compétence pour réaliser un ensemble d'activités et de tâches d'administration. Ainsi, par exemple, le demandeur « Dupont » a pour rôle (métier) administrateur de l'application de facturation : au niveau du système, le demandeur « Dupont », compte-tenu de son rôle d'administrateur de l'application de facturation, dispose des privilèges « administrateur de base de données » (« admin_db »), « super_db », « opérateur réseau », « installateur de logiciel à distance », « opérateur système ».

L'ensemble des privilèges dans un rôle donné sert de base pour contrôler les actions d'un demandeur. Un demandeur se voit attribuer un ou plusieurs rôles. Le demandeur 7 définit de nouveaux rôles ou modifient des rôles existants en ajoutant ou supprimant des privilèges.

Les listes de contrôle d'accès enregistrées dans les moyens 12 d'enregistrement définissent les conditions d'obtention de droits d'accès sur des ressources rattachées à des entités 4 les gérant : elles offrent une interface basée sur des permissions configurées.

Une permission est une association d'une ressource à un droit. Par exemple, une permission peut être d'arrêter (droit) une base de données particulière (ressource). La permission représente un type d'accès, une action ou une opération particulière dans le contexte d'une entité 4 appelante ou d'une ressource 2d de l'entité 4 appelante en question.

Les permissions sont de deux types : les permissions demandées et les permissions configurées.

- Les permissions demandées sont des questions posées par une entité 4 appelante au RAC 6. Les réponses à ces questions permettent aux entités 4 appelantes de savoir si un droit d'accès est à autoriser au demandeur dans le contexte courant d'utilisation de l'entité.
- Les permissions configurées définissent un mode d'accès possible sur une ou plusieurs ressources, comme vu plus haut. Les permissions configurées sont enregistrées dans la liste 12.

Les conditions d'obtention de permissions sont exprimées sous forme de combinaisons de privilèges.

Les listes de permissions et conditions d'obtention de ces permissions sont constituées de lignes, appelées entrées. La figure 2 représente une entrée d'une liste. L'entrée exprime les permissions configurées et les conditions d'obtention de droit sur une ressource en terme de privilèges requis. L'entrée comprend trois colonnes : une colonne droit, une colonne ressource, les colonnes droit et ressource formant la permission configurée, et une colonne privilège. Selon une forme illustrative de l'invention, la ressource est identifiée par son type ; le type est le critère de contrôle d'accès.

Les droits ou les ressources sont susceptibles d'être regroupés en groupes génériques représentés par des filtres sous forme de caractères spéciaux tels qu'une étoile « * » ou par des mots-clés tels que le mot « any ». Le mot-clé « any » signifie par exemple tout privilège. Le tableau de la figure 4 indiquent des exemples de signification du filtre étoile *. Le filtre « étoile » appliqué à un droit de format « xyz* » signifie tout droit dont le nom commence par xyz. Le filtre « étoile » appliqué à un type de ressource de format « mytype* » signifie toute ressource dont le type est mytype. Le filtre « étoile » appliqué à un chemin de ressource « /abc/def/* » signifie toute ressource dont le chemin est un sous-ensemble de /abc/def/.

Les filtres et mot-clés permettent de regrouper un grand nombre d'entrées en une seule et de faciliter de ce fait l'administration de la configuration.

Dans la forme de réalisation décrite, une entrée dans la liste représente des accès autorisés. Selon un développement de l'invention, une entrée contient également des permissions négatives.

Le système selon la présente invention permet de restreindre les ressources accessibles pour un rôle donné à une partie uniquement de l'ensemble global des ressources 2d au moyen d'un domaine de validité du rôle. Un domaine de validité définit une partie d'un ensemble de ressources 2d, accessible pour un rôle donné. Si les instances des ressources sont organisées hiérarchiquement dans un arbre, une collection de branches de ressources détermine un domaine de validité.

Une information supplémentaire relative à la nécessité de consulter le domaine de validité est prévue dans l'entrée de la liste pour éviter la comparaison systématique du domaine avec le chemin de la ressource concernée. La comparaison n'est pas nécessaire lorsque le domaine de validité correspond au chemin de la ressource. L'information en question

consiste en un booléen (oui-non) exprimant la nécessité de consulter ou pas le domaine de validité.

La figure 3 représente une liste de contrôle d'accès incluant le champ relatif à la nécessité de consulter le domaine de validité : ce champ est nommé domaine. Pour qu'un administrateur muni du privilège super-bd puisse arrêter dans la base de données, le RAC doit vérifier que le chemin de la ressource correspond au domaine de validité ce qui n'est pas le cas si l'administrateur souhaite démarrer dans la base de données. Dans ce dernier cas, l'administrateur peut démarrer toute base de données sans restriction.

Le RAC 6 attribue une valeur par défaut aux champs non renseignés d'une entrée de la liste.

Selon une forme de réalisation illustrative de l'invention, les valeurs par défaut sont :

- Pour le type de ressource : * (tout type de ressource : un droit associé au type de ressource * signifie que le droit s'applique à tout type de ressource) ;
- Pour le droit :* (tout droit : un droit * associé à une ressource signifie que tout droit s'applique à ladite ressource) ;
- Pour le domaine : oui ;
- Pour les privilèges requis : any (aucun privilège n'est requis pour le droit demandé).

Les données de sécurité d'un demandeur sont constituées d'un ou plusieurs rôles associés à un ou plusieurs privilèges et de manière optionnelle, à un domaine de validité du rôle.

Les données de sécurité d'un demandeur sont à distinguer de la liste des contrôles d'accès dans laquelle sont décrites les conditions d'obtention d'un droit sur une ressource en terme de privilèges requis et en terme de

nécessité ou pas de consulter le domaine de validité du rôle. Les données de sécurité sont enregistrées dans les moyens de stockage 10 et la liste de contrôle d'accès dans les moyens de stockage 12.

Le système selon la présente invention fonctionne de la manière suivante.

Lorsque le demandeur 7 lance l'entité 4 appelante, il sélectionne un rôle d'administration parmi ceux proposés par l'interface graphique 8 jusqu'à sa déconnexion de ladite entité 4. Dans l'exemple pris tout au long de la description qui suit, le demandeur « Dupont » est un administrateur qui sélectionne le rôle administrateur de l'application de facturation.

Le demandeur 7 demande à effectuer une action sur une ressource donnée. Par exemple, l'administrateur Dupont souhaite arrêter la base de données de facturation de Louveciennes dont le nom est « database_facturation.frlv.bull.fr ».

Lorsque l'entité 4 appelante doit décider d'autoriser ou refuser une action du demandeur 7 sur une ressource 2d déterminée, elle pose sur la base de l'identité du demandeur la question à l'API 5. L'entité 4 appelante demande une permission à l'API 5 ce qui constitue une permission demandée (comme vu plus haut).

L'entité 4 appelante soumet à l'API 5, à titre illustratif, la question suivante :

« est-ce que l'administrateur Dupont a le droit d'arrêter la ressource base de données de facturation de Louveciennes dont le nom est « database_facturation.frlv.bull.fr » ? ».

A réception de ladite question et au premier appel de l'API 5, le RAC 6 recherche le rôle et la liste des privilèges du demandeur 7 au moyen du

module 9 d'accès aux privilèges. Dans l'exemple, le demandeur 7 a notamment pour rôle « administrateur de base de données » et pour privilèges associés « super_db » et « admin-db ». Le rôle « administrateur de base de données » a pour domaine de validité les bases de données dont le nom finit par frlv.bull.fr à savoir « *.frlv.bull.fr ».

Le procédé effectue deux niveaux de contrôle, le second étant conditionnel par rapport au premier :

- un premier niveau sur les types de ressources ;
- un deuxième niveau sur l'identifiant de la ressource.

Lors du premier niveau de contrôle, le RAC 6 consulte la liste des contrôles d'accès (figure 2) à l'aide du RAD 11. Un extrait de ladite liste selon l'exemple illustré est donnée sur la figure 3. Le moteur 13 d'autorisation du RAC 6 vérifie qu'il existe au moins une entrée de la liste qui satisfait les conditions d'obtention du droit demandé, à savoir qu'elle contient les trois éléments suivant, ladite ressource, le droit demandé et l'un au moins des privilèges du demandeur.

Si les conditions d'obtention du droit ne sont pas satisfaites, à savoir qu'aucune entrée de la liste ne contiennent les trois éléments requis, le RAC 6 via l'API 5 répond par la négative à la question de l'entité 4 appelante. L'entité 4 appelante indique au demandeur 7 qu'il n'a pas le droit d'effectuer l'action demandée sur la ressource concernée, en l'espèce d'arrêter la base de données de facturation de Louveciennes.

Il est à souligner que le demandeur est informé qu'il ne peut effectuer une action déterminée sur une ressource donnée avant tout accès à ladite ressource.

Si les conditions d'obtention du droit sont satisfaites, à savoir qu'une ou plusieurs entrées de la liste contiennent simultanément les trois éléments

requis, et que par ailleurs le domaine de validité dans la ou les entrées concernées ont la valeur « non », aucun contrôle supplémentaire n'est requis. L'ensemble des ressources concernées sont accessibles pour le rôle donné. Le RAC via l'API répond par la positive à la question de l'entité 4 appelante. L'entité 4 appelante autorise le demandeur 7 d'effectuer l'action demandée, en l'espèce d'arrêter la base de données de facturation de Louveciennes.

Si les conditions d'obtention du droit sont satisfaites, à savoir qu'une ou plusieurs entrées de la liste contiennent simultanément les trois éléments requis, et que par ailleurs le domaine de validité dans la ou les entrées concernées ont la valeur « oui », le procédé passe au deuxième niveau de contrôle. C'est le cas dans l'exemple traité : la première entrée de la liste de la figure 3 satisfait les conditions d'obtention du droit demandé par l'administrateur : le droit est celui d'arrêter, le type de ressource est une base de donnée et le privilège requis est super_db.

Lors du deuxième niveau de contrôle, afin de déterminer si le rôle en question peut effectuer l'action requise sur ladite ressource, le moteur 13 d'autorisation réalise un contrôle sur le domaine de validité associé au rôle courant si les trois conditions suivantes sont réunies :

- la permission demandée contient un identifiant de ressource (nom, chemin) ; en effet, si le demandeur souhaite démarrer une base de données, la réponse ne peut qu'être négative, aucune base de données n'étant spécifiée. En revanche, si le demandeur souhaite démarrer la base de données de facturation de Louveciennes, une réponse peut être apportée suivant le rôle et les privilèges du demandeur ;
- il existe au moins une permission configurée qui correspond à la permission demandée ; le RAC utilise le critère de contrôle d'accès pour identifier une ressource afin d'effectuer la comparaison des permissions demandées aux permissions configurées ;

- le champ consultation du domaine de validité a pour valeur oui, ce qui signifie qu'il faut vérifier le domaine de validité, l'action étant restreinte à un sous-ensemble de la totalité des ressources. Lorsqu'un domaine de validité est associé à un rôle et que le champ consultation du domaine de validité a pour valeur oui, tout demandeur disposant de ce rôle n'accède ou n'agit que sur des ressources du domaine de validité

Si les trois conditions sont réunis, le RAC 6 compare l'identifiant de la ressource dans la question posée au domaine de validité du rôle retrouvé dans les moyens de stockage 10 par le module 9 comme vu plus haut.

Si le domaine de validité ne correspond pas à la ressource en question, les conditions d'obtention du droit ne sont pas remplies et le RAC 6 répond à l'entité 4 appelante via l'API 5 que l'utilisateur n'a pas le droit de réaliser l'action demandée.

Si le domaine de validité correspond à la ressource en question, les conditions d'obtention du droit sont remplies et le RAC 6 répond à l'entité 4 appelante via l'API 5 que l'utilisateur a le droit de réaliser l'action demandée.

Dans l'exemple de la description, le procédé compare la ressource base de données de facturation de Louveciennes dont le nom est « database_facturation.frlv.bull.fr » au domaine de validité du rôle administrateur de base de données qui est constitué des bases de données dont le nom finit par frlv.bull.fr à savoir « *.frlv.bull.fr ». La ressource base de données de facturation de Louveciennes a un nom qui finit par frlv.bull.fr : elle appartient donc au domaine de validité. L'entité 4 appelante autorise l'administrateur 7 à arrêter la base de données de facturation de Louveciennes.

Il est à souligner que :

- les permissions sont indépendantes des demandeurs : les permissions sont accordées ou refusées suivant le rôle et les privilèges du demandeur ;
- le contrôle d'accès ne nécessite pas d'accès physique aux ressources : un filtrage d'actions est réalisé avant tout accès ;
- le dispositif de contrôle d'accès est rapide. De plus, le dispositif et le procédé selon l'invention offrent une optimisation du contrôle d'accès.

La présente invention concerne le procédé de contrôle d'accès du demandeur 7 à des ressources 2d dans le système informatique 1, caractérisé en ce qu'il consiste à définir des rôles recouvrant un ou plusieurs privilèges et représentant une compétence du demandeur pour réaliser des tâches spécifiques, à enregistrer les rôles définis dans les moyens 10,12 de stockage, et à enregistrer la liste de contrôle d'accès définissant les conditions d'obtention d'un droit sur un type de ressource, à savoir d'une permission configurée en terme de privilèges dans lesdits moyens 10,12.

Le procédé effectue le contrôle d'accès du demandeur 7 à des ressources 2d sans accéder auxdites ressources 2d.

Le procédé effectue un contrôle d'accès à deux niveaux :

- un premier sur le type des ressources 2d ;
- un deuxième niveau sur l'identifiant des ressources 2d.

Le procédé consiste à :

- identifier le demandeur ainsi que son rôle et ses privilèges ;
- comparer les privilèges et les permissions demandées par le demandeur avec les privilèges requis et permissions configurées enregistrés dans les moyens 10 de stockage et ;

- autoriser l'action requise sur la ressource concernée lorsque des permissions demandées et configurées correspondent et que l'un des privilèges requis correspond au privilège de l'entité.

Le procédé consiste à restreindre à une partie des ressources seulement les ressources accessibles pour un rôle donné au moyen d'un domaine de validité, et à enregistrer les domaines de validité constitués dans les moyens de stockage 10.

Le procédé consiste à consulter une information enregistrée dans les moyens de stockage 10 relative à la nécessité de consulter le domaine de validité et à vérifier que la ressource concernée appartient au domaine de validité seulement si ladite information le requiert.

Le procédé consiste à regrouper des droits ou des ressources en groupes génériques représentés par des caractères spéciaux ou mots-clés ou autres.

La présente invention concerne également le dispositif susceptible de mettre en œuvre le procédé décrit ci-dessus.

La présente invention se rapporte au dispositif de contrôle d'accès du demandeur à des ressources 2d dans le système informatique 1, caractérisé en ce qu'il comprend la machine 2a d'administration comportant le service de contrôle d'accès, le RAC 6 et les moyens de stockage 10 de rôles, privilèges et listes de contrôle d'accès.

REVENDICATIONS

1. Procédé de contrôle d'accès d'un demandeur (7) à des ressources (2d) dans un système informatique (1) dans lequel le demandeur se voit attribuer un ou plusieurs rôles, basé sur une liste de contrôle d'accès définissant les conditions d'obtention d'un droit sur une ressource, caractérisé en ce qu'il consiste à restreindre à une partie des ressources seulement les ressources accessibles pour un rôle donné au moyen d'un domaine de validité du rôle.

2. Procédé selon la revendication 1, caractérisé en ce qu'il enregistre une information supplémentaire relative à la nécessité de consulter le domaine de validité du rôle dans la liste de contrôle d'accès.

3. Procédé selon la revendication 2, caractérisé en ce qu'il consulte l'information supplémentaire relative à la nécessité de consulter le domaine de validité du rôle et vérifie que la ressource concernée appartient au domaine de validité seulement si ladite information le requiert.

4. Procédé selon la revendication 2, caractérisé en ce qu'il effectue un contrôle d'accès à deux niveaux :

- un premier sur le type des ressources (2d) ;
- un deuxième niveau sur l'identifiant des ressources (2d).

5. Procédé selon la revendication 4, caractérisé en ce qu'il effectue un premier niveau de contrôle en vérifiant l'existence d'au moins une entrée de la liste de contrôle d'accès qui vérifie les conditions d'obtention du droit demandé et si l'entrée existe, l'existence d'un domaine de validité pour ladite entrée.

6. Procédé selon la revendication 5, caractérisé en ce qu'il effectue un deuxième niveau de contrôle en vérifiant si la permission demandée contient un identifiant de ressource, l'existence d'au moins une permission configurée

correspondant à la permission demandée, et la valeur de l'information supplémentaire relative à la nécessité de consulter le domaine de validité.

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce qu'il consiste à regrouper des droits ou des ressources en groupes génériques représentés par des caractères spéciaux ou mots-clés ou autres.

7. Dispositif de contrôle d'accès d'un demandeur à des ressources (2d) dans un système informatique (1), caractérisé en ce qu'il comprend une machine (2a) d'administration comportant un service de contrôle d'accès, le RAC (6) et des moyens de stockage (10) de rôles, listes de contrôle d'accès et domaines de validité.

8. Dispositif permettant la mise en œuvre du procédé selon l'une des revendications 1 à 6.

9. Module logiciel permettant la mise en œuvre du procédé selon l'une des revendications 1 à 6.

ABREGE DESCRIPTIF

La présente invention concerne un procédé de contrôle d'accès d'un demandeur (7) à des ressources (2d) dans un système informatique (1), consistant à définir des rôles recouvrant un ou plusieurs privilèges et représentant une compétence du demandeur pour réaliser des tâches spécifiques, à enregistrer les rôles définis dans des moyens (10,12) de stockage, et à enregistrer une liste de contrôle d'accès définissant les conditions d'obtention d'un droit sur un type de ressource, à savoir d'une permission configurée en terme de privilèges dans lesdits moyens (10,12).

La présente invention concerne également le dispositif de mise en œuvre dudit procédé.

Figure de l'abrégé : Figure 1

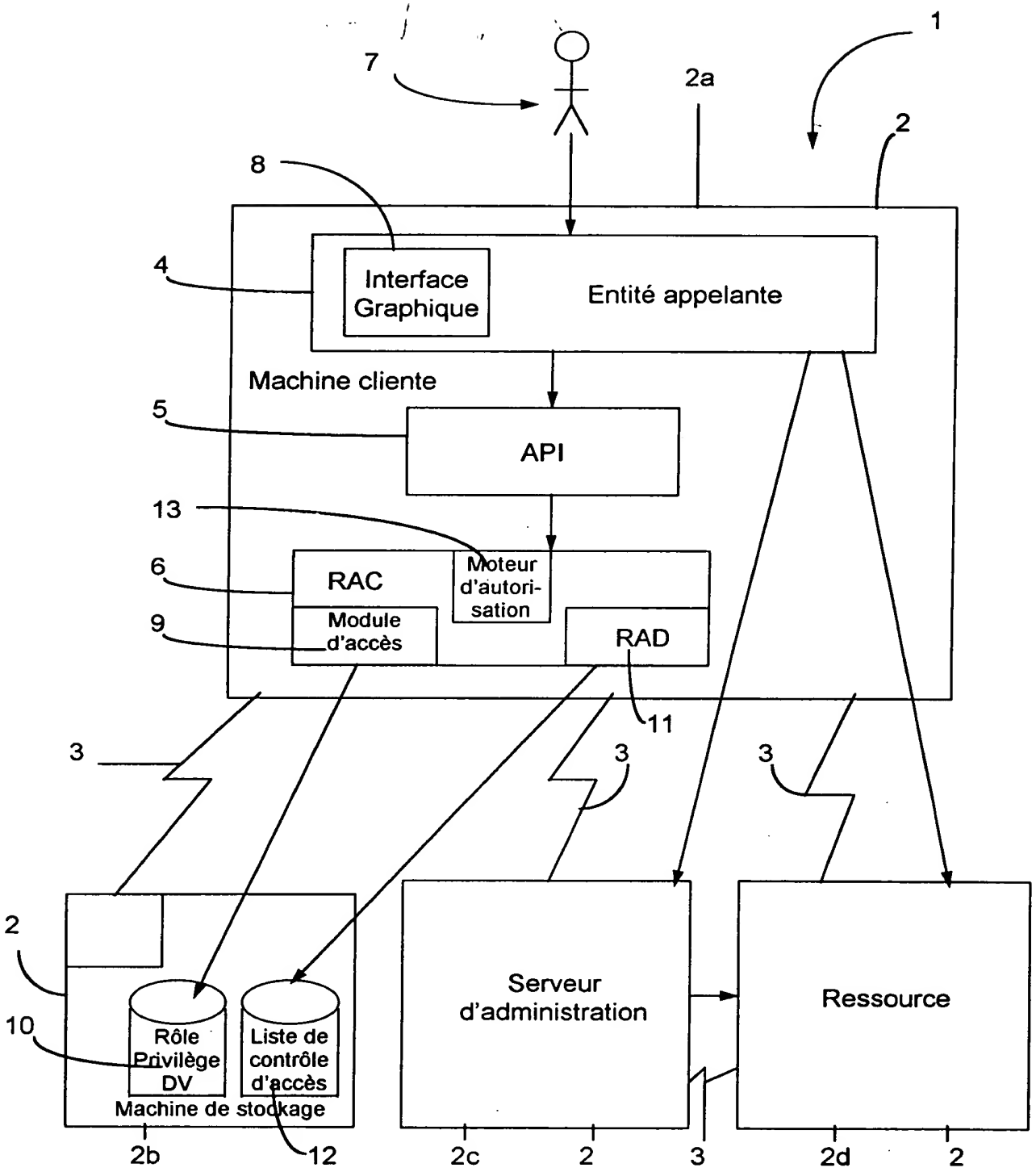
1
7
2a
2
8
4
Interface Graphique
Entité appelante
Machine cliente
5
API
13
6
RAC
Moteur d'autori-sation
9
Module d'accès
RAD
11
3
3
3
2
10
Rôle Privilège DV
Liste de contrôle d'accès
Machine de stockage
Serveur d'administration
Ressource
2b
12
2c
2
3
2d
2

FIG.1

Permission configurée		Domaine	Privilèges requis
Droit	Type de ressource	oui/non	Privilège1/Privilège2/.../Privilègen

FIG.2

Droit	Ressource	Domaine	Privilège
arrêter	base de données	oui	super-db
démarrer	base de données	non	admin-db/super-db

FIG.3

Colonne	Caractère	Format	Signification
Droit	*	« xyz* »	tout droit, dont le nom commence par xyz
Type de ressource	*	« mytype* »	toute ressource dont le type est mytype
Chemin ressource	*	« /abc/def/* »	toute ressource dont le chemin est un sous-ensemble de /abc/def/

FIG.4

FIGURE DE L'ABREGE